Acquiring Secure Systems Through Information Economics

Chad Dacus
Research Professor of Defense Economics
Air Force Research Institute

Dr. Pano Yannakogeorgos
Research Professor & Deputy Director
Air University Cyber Research Task Force

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Acquiring Secure Systems Through Information Economics	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute,Maxwell AFB,AL,36112-6026**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 12th Annual Acquisition Research Symposium held May 13-14, 2015 in Monterey, CA.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**15**	

Introduction

"For all future weapons systems that DoD will acquire or procure, DoD will mandate specific cybersecurity standards for weapons systems to meet. Acquisition and procurement policy and practice will be updated to promote effective cybersecurity throughout a system's life cycle."

- **DOD moving toward holding contractors liable**
- **Is now the best time to add contractor risk?**
- **Is this enough?**
  - **Minimum standard**
  - **Dynamic adversaries**

Dynamic Adversaries

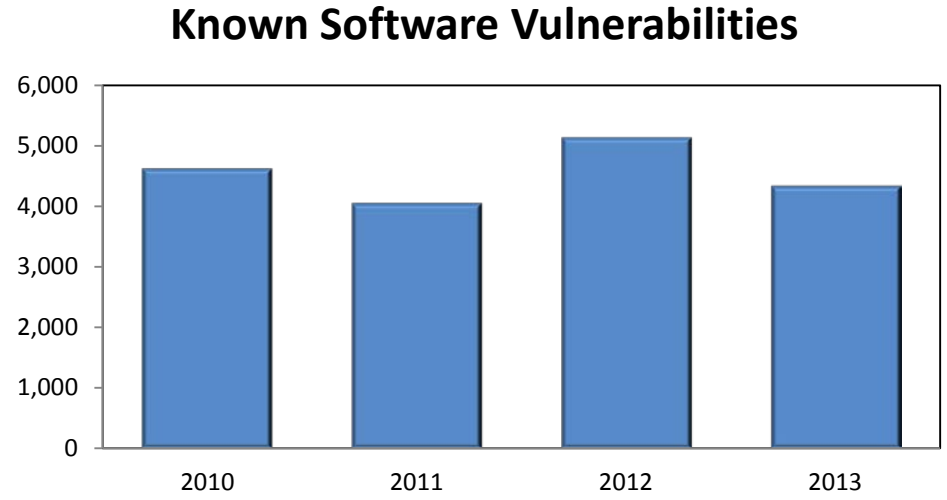
Foreign Intelligence

Traditional Military

Criminal

Ad Hoc

Cyber Risk to Military Missions



- If adversary can hack into mission essential software/hardware, then mission is compromised
- Mission assurance requires materiel solutions, educated personnel (acquisition & operators), and TTPs

Disruption ← → Failure

Degree of mission compromise

Duration of compromise may range from seconds to days, months, or years

Spectrum of Cyber Operations

Access Operations
• Digital intelligence (e.g., stealthy implant)

Disruption
•Interrupt the flow of information or function of information systems without physical damage or injury

Attack
• Use of force
• Physical damage or destruction
• Physical injury or death

Very stealthy — Less stealthy

Motivating Contractor Efforts

- Contractors have different priorities than the DOD when it comes to cybersecurity
  - Classic example
    - Manager's huge office
  - In another defense context
    - Cost-reimbursement contracts

  - Why is this the case?
    - Contractor can satisfy client through other achievements
    - DOD has not clearly communicated importance

Motivating Contractor Efforts

- Government's problem: Outcomes to avoid?
  - Minimize:
    - Expected payments to contractors plus
    - Expected cost of hacking
  - Subject to:
    - Contractor participation constraint
    - Contractor chooses government's favored level of effort
  - Results
    - Fee for successful protection
    - Penalty for breach

Motivating Contractor Efforts

- Implications
  - Incentives Depend on:
    - Probability of success
    - Marginal cost of effort
    - Marginal benefit of effort
  - Need a more functional way to set incentives
- How to administer incentives?
  - Incentive fees
  - Award fees

Choosing the Right Contractors

- Less expensive contractors likely to win contract over those with strong cybersecurity commitment and practices
  - Classic example:
    - “Market for Lemons”
  - In another defense context:
    - Sealed bids
  - Why is this the case?
    - Cybersecurity is considered a constraint
    - Cybersecurity is costly to provide

Choosing the Right Contractors

- What to do about it?
  - Screening
    - Actively consider cybersecurity when awarding contract
    - Difficult when you have so many objectives
  - Encourage signaling
    - Foster metric development

Choosing the Right Contractors

- More specifically
  - Screen by system sensitivity
    - Boost incentives
    - Require higher quality scores
  - Quality scores
    - Historical system protection
    - Vulnerability Assessment/Penetration Testing
      - Weakness and Vulnerability scores
        - How to aggregate?

Effectiveness of Incentives?

- Long history of incentives in DOD

- Empirical results
  - GAO (1999-2003)
    - Incentives not particularly helpful
    - Recommendations

  - 2014 Performance of DOD Acquisition System
    - Incentive contracts performed at least as well

Concerns

- Detection Lag and Uncertainty
  - Alternate signals
- Adversarial behavior
- Setting appropriate fee
  - Budget buster
  - Tradeoffs

Conclusions

- Move beyond a compliance mindset

- Economic theory calls for cybersecurity incentives
  - Truly makes cybersecurity a priority
  - Size based on system sensitivity
  - Monitor profit margins/perverse behavior

- Lack of metrics is an obstacle
  - Encourage creativity through rewards
  - Information sharing important

Questions?

Dr. Chad Dacus
Research Professor & Chief Economist
Air Force Research Institute
Chad.Dacus@us.af.mil

Dr. Pano Yannakogeorgos
Research Professor & Deputy Director
Air University Cyber Research Task Force
Panayotis.Yannakogeorgos@us.af.mil